What is claimed is:

CLAIMS

1. A method for remote administration of at least one smart card via a communication network, the method comprising:

associating said at least one smart card with a remote administrator by storing administrator identification information of the remote administrator in said at least one smart card;

inserting said at least one smart card in at least one user unit;

employing the administrator identification information stored in said at least one smart card to identify the remote administrator associated with said at least one smart card; and

establishing communication between the at least one smart card and the remote administrator via the communication network in accordance with the administrator identification information.

2. A method according to claim 1 and wherein said establishing step is performed via said at least one user unit.

3. A method according to claim 1 and wherein said establishing step comprises employing Internet Protocol (IP) for communication via the communication network.

4. A method according to claim 1 and wherein said establishing step comprises the steps of:

identifying a local administrator other than the remote administrator, the local administrator being positioned in the communication network in a proximity to said at least one user unit; and

determining the local administrator as a proxy administrator for administrating said at least one smart card by transmitting at least authorization information from the remote administrator to the local administrator.

5. A method according to claim 1 and also comprising the step of administrating said at least one smart card after communication with the remote administrator is established.

6. A method according to claim 5 and wherein said administrating step comprises the step of administrating said at least one smart card immediately after communication with the remote administrator is established.

7. A method according to claim 4 and also comprising the step of administrating said at least one smart card immediately after communication with the proxy administrator is established.

8. A method according to claim 7 and wherein said administrating step comprises the step of administrating said at least one smart card immediately after communication with the proxy administrator is established.

9. A method according to claim 5 and wherein said administrating step comprises performing an administration initialization procedure to at least one of authenticate, verify and validate said at least one smart card.

10. A method according to claim 9 and also comprising the step of preventing performance of any operation other than the administration initialization procedure until said administration initialization procedure is verified to be in order.

11. A method according to claim 1 and wherein said step of employing the administrator identification information to identify the remote administrator comprises the step of identifying the at least one smart card in a smart card data base at the remote administrator.

12. A method according to claim 1 and also comprising the step of accessing a protected information resource by said at least one smart card via the remote administrator associated therewith.

13. A method according to claim 12 and wherein said accessing step comprises performing at least one administration operation.

14. A method according to claim 13 and wherein said at least one administration operation comprises at least one of the following: transmission of a certificate; transmission of credentials; transmission of a key; renewal of said at least one smart card; expiration date updating; renewal of an authorization to said at least one smart card; validity check of data in said at least one smart card; integrity check of data in said at least one smart card; memory load/check; revocation of at least one of an authorization, a certificate and a smart card; execution of a "KILL CARD" process after a verification of a need to prevent operation of said at least one smart card; data load; and transmission of smart card chaining information.

15. A method according to claim 12 and wherein said accessing step comprises the step of performing security mechanisms for accessing the protected information resource by said at least one smart card.

16. A method according to claim 15 and wherein said security mechanisms include at least one of the following: unilateral or bilateral authentication; time stamping; non-repudiation; digital signatures; distribution of an encryption key; change of an encryption key; encryption; and password authorization.

17. A method according to claim 12 and wherein each operation performed during said accessing step by at least one of said remote administrator and said at least one smart card is performed only upon receipt of an "END

ADMINISTRATION OPERATION" instruction at a corresponding one of said at least one of said remote administrator and said at least one smart card.

a1

18. A method according to claim 12 and wherein said remote administrator comprises a plurality of administrators, each operative to perform at least part of said step of accessing the protected information resource and/or at least part of an administration initialization procedure.

19. A method according to claim 1 and wherein said communication network comprises at least one of the following: a local-area-network (LAN); a metropolitan-area-network (MAN); and a wide-area-network (WAN).

20. A secure access method for use with a communication network which communicates information between an information resource controller and a remote unit, the method comprising:

identifying, at the remote unit, a command to upload data;

employing, in response to said command, a hash function at the remote unit to encode contents of at least a portion of a memory at the remote unit and thereby to produce a hashed result;

transmitting the hashed result to the information resource controller;

comparing, at the information resource controller, the hashed result with a trusted hashed result maintained at the information resource controller thereby to provide a comparison result; and

determining integrity of the contents of the at least a portion of the memory at the remote unit based, at least in part, on the comparison result.

21. A method according to claim 20 and wherein said determining step comprises the step of transmitting repairing information to the remote unit to correct the contents of said at least a portion of the memory at the remote unit if the comparison result is unfavorable.

22. A method according to claim 20 and wherein said command is generated at the remote unit periodically.

23. A method according to claim 20 and wherein said command is transmitted from the information resource controller to the remote unit periodically.

24. A method according to claim 20 and wherein said command is generated at the remote unit following a communication failure event.

25. A method according to claim 20 and wherein said command is transmitted from the information resource controller to the remote unit following a communication failure event.

26. A method for remote administration of a first smart card and a second smart card via a communication network, the method comprising:

associating said first smart card and said second smart card with a remote administrator; and

transmitting authorization information from said first smart card to said second smart card via the remote administrator and the communication network.

27. A method according to claim 26 and wherein said authorization information comprises at least one of the following: administrator identification information; authorization to perform a transaction; an electronic-mail message stored in said first smart card; and billing history information.

28. A method according to claim 26 and wherein said communication network comprises at least one of the following: a local-area-network (LAN); a metropolitan-area-network (MAN); and a wide-area-network (WAN).

29. A method according to claim 26 and wherein said communication network comprises at least one of the following networks: the Internet; CompuServe; and America-On-Line.

30. A remote administrator for administrating at least one smart card via a communication network, the remote administrator comprising:

a processor comprising:

an access control module operative to control access to a protected information resource; and

a data base module operative to map said at least one smart card to an access control list.

31. Apparatus according to claim 30 and also comprising:

a memory operative to store a log of the communication network activity.

32. Apparatus according to claim 30 and also comprising:

communication apparatus for transmitting authorization information from a first smart card associated with the remote administrator to a second smart card associated with the remote administrator via the communication network.

33. A system for remote administration of at least one smart card via a communication network, the system comprising:

a remote administrator having administrator identification information;

at least one user unit; and

at least one smart card associated with said remote administrator by storing in the at least one smart card said administrator identification information of the remote administrator, wherein

said at least one smart card inserted in said at least one user unit is operative to employ the administrator identification information to identify the

remote administrator associated with said at least one smart card, and to establish communication via the communication network between the at least one smart card and the remote administrator in accordance with the administrator identification information.

34. A system for providing secure access in a communication network comprising:

a remote unit operative to identify a command to upload data, and to employ, in response to said command, a hash function to encode contents of at least a portion of a memory associated with the remote unit thereby to produce a hashed result; and

an information resource controller operatively associated with said remote unit and operative

to receive, from said remote unit, the hashed result,

to compare the hashed result with a trusted hashed result maintained at the information resource controller thereby to provide a comparison result, and

to determine integrity of the contents of the at least a portion of the memory based, at least in part, on the comparison result.